Privacy Policy - Candidates

1. INTRODUCTION

1.1 finnCap Ltd is committed to ensuring that your privacy is protected. This privacy policy explains how we process personal information concerning candidates who apply for roles with finnCap ("**you**", "**your**").

1.2 This policy sets out what personal information we collect, why we collect it, how we use it and the legal basis for doing so and the procedures we have in place to protect your personal information. It is important to read this policy, together with any other privacy policy we may provide in specific circumstances when we are processing your personal information, so that you are aware of how and why we are using your information.

1.3 This policy does not form part of any contract of employment or other contract for services and may be amended at any time.

2. ABOUT FINNCAP LTD

2.1 We are finnCap Ltd, a limited liability company registered in England and Wales under number 06198898. Our registered office is at 60 New Broad Street, London, EC2M 1JJ.

2.2 finnCap is a data controller of the personal information of its Staff and candidates. This means that we are responsible for deciding how we hold and use personal information about you.

2.3 We are registered with the Information Commissioner's Office ("**ICO**") under registration number Z9884968.

2.4 finnCap Ltd is authorised and regulated by the Financial Conduct Authority ("**FCA**").

2.5 References in this Policy to "finnCap", "we", "our" and "us" are references to finnCap Ltd, the UK data controller.

2.6 finnCap's Data Privacy Manager is Mark Tubby.

Questions about your personal information:
If you have any questions about this privacy policy or your information, or to exercise any of your rights as described in this policy or under applicable data protection laws, you can contact us at:
The Privacy Manager
finnCap Ltd
60 New Broad Street
London, EC2M 1JJ
By email: PrivacyManager@finnCap.com
By telephone: +44 (0)20 7220 0500

3. DATA PROTECTION PRINCIPLES

3.1 Anyone processing personal information must comply with the principles of processing personal information. We set out these principles below along with our procedures for complying with such principles:

- Lawfulness, fairness and transparency – data must be processed lawfully, fairly and in a transparent manner.
- Purpose limitation - data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Data minimisation - data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accuracy - data must be accurate and, where necessary, kept up to date.
- Storage limitation - data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal information are processed.
- Integrity and confidentiality - data must be processed in a manner that ensures appropriate security of the personal information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage by using appropriate technical or organisational measures.

4. WHAT INFORMATION WE COLLECT

4.1 We collect personal information from our candidates to assist with our recruitment processes and to monitor recruitment statistics.

4.2 We set out below a list of the categories of information we may collect from candidates. We aim to make this list as comprehensive as possible but it is not exhaustive. The information that we may collect includes, but is not limited to, the following:

- personal contact details such as name, title, home address, telephone number and email address;
- date of birth;
- gender;
- copies of passport, driving licence and similar documents;
- education history, training and professional experience;
- current and past employment details;
- immigration status and work permits;
- languages spoken and level of proficiency;
- other information given in your CV;
- right to work documentation;
- references;
- your photograph; and
- data from building access controls including images from CCTV operating in and around our offices.

5. INFORMATION PROVIDED BY THIRD PARTIES

5.1 We collect personal information about our candidates from the following third party source:

5.1.1 Vero Screening, from which we collect the following categories of data: employment history, recent address history, directorships, professional and other qualifications.

5.1.2 Insights Discovery, from which we collect your personal colour profile.

5.1.3 The FCA website, which is publicly accessible, from which we collect your FCA registration number and approval category listing.

6. SPECIAL CATEGORIES OF ("SENSITIVE") PERSONAL INFORMATION

6.1 You may also supply us with, or we may receive, sensitive personal information relating to your racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or data concerning your health or data concerning your sex life or sexual orientation, genetic and biometric data.

6.2 We will use this information for the purposes of either performing our contractual obligations or exercising obligations or rights which are imposed or conferred on us by law in connection with our obligations as an employer including:

- diversity information about your race or ethnic origin, religious beliefs or sexual orientation for monitoring of equality of opportunity or treatment;
- information about your disability status for considering whether adjustments may need to be made to accommodate candidates with a disability;
- reporting and maintaining a record of any accidents at work.

6.3 We process these special categories of personal information on the basis of one or more of the following:

6.3.1 where the processing is necessary for carrying out obligations in the employment field;

6.3.2 where you have given explicit consent to the processing of the personal information for one or more specified purposes;

6.3.3 where the processing relates to personal information which is manifestly made public by you;

6.3.4 where the processing is necessary for reasons of substantial public interest in accordance with applicable law. This includes where the processing is necessary for equality of opportunity of treatment; and

6.3.5 where the processing is necessary for the establishment, exercise or defence of legal claims.

7. DATA RELATING TO CRIMINAL CONVICTIONS & OFFENCES

7.1 We also collect, store and otherwise process personal information relating to criminal convictions and offences (including the alleged commission of offences) for the purposes of either performing our contractual obligations or exercising our obligations as an employer and specifically to assess our suitability for the role (where appropriate).

7.2 This information will be processed on the basis of one or more of the following:

7.2.1 the processing is necessary for exercising obligations or rights in connection with employment;

7.2.2 the processing is necessary for reasons of substantial public interest in accordance with applicable law. This includes where the processing is necessary:

7.2.2.1 for equality of opportunity of treatment;

7.2.2.2 for the purposes of the prevention or detection of an unlawful act or for preventing fraud.

7.2.2.3 for the purposes of complying with a regulatory requirement, which involves a person taking steps to establish whether another person has committed an unlawful act or been involved in dishonesty, malpractice or other seriously improper conduct.

7.2.3 the processing is necessary for the purposes of, or in connection with any legal proceedings (including prospective legal proceedings), or necessary for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.

8. WHAT WE DO WITH YOUR INFORMATION

8.1 The information about you which is obtained by us during the application process and during the course of your employment or contract for services (whether obtained directly from you or from third parties) may be used by us for the following purposes:

- to consider your suitability for employment or consultancy services;
- to take up your references;
- to conduct appropriate checks;
- to negotiate and communicate with you in relation to your application;
- to manage and operate our business and for administrative purposes;
- to undertake business analysis activities; and
- to comply with our legal and regulatory obligations and for other legal purposes.

9. THE LEGAL BASIS FOR OUR PROCESSING

9.1 The legal basis for our processing of your personal information is based on the fact that you are Staff or a candidate and it is necessary for us to process your information in order to:

Purposes for which we will process the information	**Legal Basis for the processing**
To consider your application in line with our recruitment purposes;	It is in our legitimate interests to recruit Staff and to select the best candidates. We consider this to be necessary for our legitimate interests and will not be prejudicial or detrimental to you.
To carry out background and reference checks;	It is in our legitimate interests to assess the suitability of candidates. We consider this to be proportionate and will not be detrimental to you.
To undertake business analysis activities;	It is in our legitimate interests to manage and monitor our Human Resources function. We consider this to be necessary for our legitimate interests and will not be prejudicial or detrimental to you.
To comply with our legal and regulatory obligations;	It is necessary to comply with our legal and statutory obligations as an employer and service provider.

9.2 Where we rely on legitimate interests as a lawful basis, we will carry out a balancing test to ensure that your interests, rights and freedoms do not override our legitimate interests. Where you provide consent, you can withdraw your consent at any time and free of charge, but without affecting the lawfulness of processing based on consent before its withdrawal. You can update your details or change your privacy preferences by contacting our Privacy Manager as provided above.

9.3 If you choose not to provide information requested, which is necessary for us to assess your suitability for roles (such as evidence of qualifications or work history), we will not be able to take your application further.

9.4 finnCap will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you in a timely manner and we will explain the legal basis which allows us to do so.

10. SHARING YOUR INFORMATION WITH THIRD PARTIES

10.1 For the purposes set out in sections 8 and 9 above, we may share information concerning candidates with other authorised Staff.

10.2 We will also disclose personal information concerning candidates to other third parties where there is a legitimate reason to do so including for the following reasons:

- in the event that we sell or buy any business or assets, in which case we may disclose your personal information to the prospective seller or buyer of such business or assets;
- if all or substantially all of our assets are acquired by a third party, in which case personal information held by it about its employees will be one of the transferred assets.

10.3 We will also disclose your personal information to the extent we are under a duty to disclose or share your personal information in order to comply with any legal obligation.

11. ACCURACY OF DATA

11.1 We will take reasonable steps to try to ensure that your information is kept accurate and up-to-date. All candidates are requested to ensure that Human Resources are notified of any changes to their personal information without undue delay.

11.2 Where you have notified Human Resources or we otherwise become aware of an inaccuracy in your personal information, we will take every reasonable step to sure that the information is either erased or rectified without delay.

12. YOUR RIGHTS

12.1 Subject to certain limitations, you have the following rights under data protection laws in relation to your personal information:

12.2 *Access to your information and updating your information*

12.2.1 You have the right to access information which we hold about you. If you so request, we shall provide you with a copy of your personal information which we are processing ("subject access request"). We may refuse to comply with a subject access request if the request is manifestly unfounded or excessive or repetitive in nature.

12.2.2 You also have the right to receive your personal information in a structured and commonly used format so that it can be transferred to another data controller ("data portability"). This right only applies where your personal data is processed by us with your consent or for the performance of a contract and when processing is carried out by automated means.

12.2.3 We endeavour to ensure that your personal information is accurate and up to date and you have the right to have inaccurate personal information rectified, or completed if it is incomplete. We may refuse to comply with a request for rectification if the request is manifestly unfounded or excessive or repetitive.

12.3 *Right to object*

12.3.1 You have the right to object at any time to our processing of your personal information used for direct marketing purposes.

12.4 *Where we process your information based on our legitimate interests*

12.4.1 You also have the right to object, on grounds relating to your particular situation, at any time, to processing of your personal information which is based on our legitimate interests. Where you object on this ground, we shall no longer process your personal information unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

12.5 *Your other rights*

12.5.1 You also have the following rights under data protection laws to request that we rectify your personal information which is inaccurate or incomplete.

12.5.2 In certain circumstances, you have the right to:

12.5.2.1 request the erasure of your personal information ("right to be forgotten");

12.5.2.2 restrict the processing of your personal information to which you have given us your consent or used for the establishment, exercise or defence of legal claims or used for the protection of the rights of others.

12.5.3 Please note that the above rights are not absolute, and we may be entitled to refuse requests, wholly or partly, where exceptions under applicable law apply. We may refuse a request for erasure, for example, where the processing is necessary to comply with a legal obligation or necessary for the establishment, exercise or defence of legal claims. We may refuse to comply with a request for restriction if the request is manifestly unfounded or excessive or repetitive in nature.

13. EXERCISING YOUR RIGHTS

13.1 You can exercise any of your rights as described in this policy and under data protection laws by contacting the Privacy Manager.

13.2 Save as provided under applicable data protection laws, there is no charge for the exercise of your legal rights. However, if your requests are manifestly unfounded or excessive, in particular because of their repetitive character, we may either: (a) charge a reasonable fee (subject to any limits imposed by applicable law) taking into account the administrative costs of providing the information or taking the action requested; or (b) refuse to act on the request.

13.3 Where we have reasonable doubts concerning the identity of the person making the request, we may request additional information necessary to confirm your identity.

14. DATA SECURITY

14.1 We store your personal information in hard copy and electronic format. We use appropriate technical and organisational safeguards to protect personal information both online and offline from unauthorised use, loss or destruction. We use industry standard physical and procedural security measures to protect information from the point of collection to the point of destruction. This includes encryption, pseudonymisation, firewalls, access controls, policies and other procedures to protect information from unauthorised access.

14.2 Only authorised personnel and third party service providers are permitted access to personal information, and that access is limited by need. We will only transfer personal information to a third party if it agrees to comply with those procedures and policies, or if it puts in place adequate measures itself.

14.3 Despite these precautions, however, finnCap cannot guarantee the security of information transmitted over the Internet or that unauthorised persons will not obtain access to personal information. In the event of a data breach, finnCap have put in place procedures to deal with any suspected breach and will notify you and any applicable regulator of a breach where required to do so.

15. INTERNATIONAL TRANSFERS

15.1 It is sometimes necessary for us to transfer and store your personal data outside the European Economic Area ("**EEA**") as follows:

15.1.1 with our service providers located outside the EEA;
15.1.2 if you are based outside the EEA.

15.2 Where personal data is transferred to and stored outside the EEA, we take steps to provide appropriate safeguards to protect your personal data, including:

15.2.1 transferring your personal data to a country, territory, sector or international organisation which the European Commission has determined ensures an adequate level of protection, as permitted under Article 45(1) GDPR;
15.2.2 entering into standard contractual clauses approved by the European Commission, obliging recipients to protect your personal data as permitted under Article 46(2)(c) GDPR;
15.2.3 under the EU-U.S. Privacy Shield Framework which enables U.S. business to self-certify as a means of complying with EU data protection laws;

15.3 In the absence of an adequacy decision or of appropriate safeguards as referenced in 15.2 above, we will only transfer personal data to a third country where one of the following applies (as permitted under Article 49 GDPR)):

15.3.1 the transfer is necessary for the performance of our contractual engagement with you;
15.3.2 the transfer is necessary for the establishment, exercise or defence of legal claims; or
15.3.3 you have provided explicit consent to the transfer.

15.4 If you want further information on the specific mechanism used by us when transferring your personal data out of the EEA, please contact our Privacy Manager using the details set out above.

16. HOW LONG WE KEEP YOUR INFORMATION

16.1 For candidates, if your application is successful and you subsequently become employed by us, the information will become part of your personnel file and our staff privacy policy will be made available to you.

16.2 Personal information about unsuccessful candidates will be deleted six months after the recruitment exercise has been completed. We may retain de-personalised statistical information about applicants to help inform our recruitment activities, but no individuals are identifiable from that data.

17. COMPLAINTS

17.1 If you have concerns about our use of your personal information, please send an email with the details of your complaint to our Privacy Manager using the details above.

17.2 You have the right to make a complaint at any time with a supervisory authority, in particular in the EU (or EEA) state where you work, normally live or where any alleged infringement of data protection laws occurred. The supervisory authority in the UK is ICO who may be contacted at https://ico.org.uk/concerns/ or telephone: 0303 123 1113.

18. UPDATES TO THIS PRIVACY POLICY

18.1 This policy will be reviewed and, if appropriate, updated from time to time. We will communicate any policy updates by email or any other appropriate method.

18.2 This privacy policy was last reviewed and updated on **25 May 2018.**